

AI and IoT: Transforming Smart Home Technology

A Unified Framework for Adaptive Automation, Sustainable Energy Management, and Intelligent Security

Ajeet Kumar, Ali Shekh Ali, Ali Ali

¹Department of Computer Science & IT, JAIN (Deemed to be University), Bengaluru, Karnataka

²Department of Computer Science & IT, JAIN (Deemed to be University), Bengaluru, Karnataka

³Department of Computer Science & IT, JAIN (Deemed to be University), Bengaluru, Karnataka

Article Info

Keywords:

Smart Home System
Artificial Intelligence
Internet of Things
Home Automation
LSTM Neural Network
Energy Optimization
Predictive Security
MQTT Protocol
Random Forest
IoT Sensors

ABSTRACT

Contemporary residential living is undergoing a fundamental technological transformation, driven by converging advances in Artificial Intelligence (AI) and the Internet of Things (IoT). This paper introduces the Smart Home Transformation System (SHTS)—a comprehensive five-tier AI-IoT framework engineered to unify adaptive device automation, real-time energy conservation, and data-driven security surveillance within a single deployable architecture. The sensing tier deploys eight distinct IoT modalities spanning thermal, luminous, kinetic, chemical, and electrical domains, whose outputs are aggregated at a Raspberry Pi 4B gateway and relayed via MQTT to a cloud-resident intelligence engine. The AI tier comprises three specialized sub-systems: a Random Forest occupancy classifier achieving 94.7% accuracy, a two-layer LSTM network for anticipatory behavioral modeling with 87.3% prediction accuracy, and an Isolation Forest anomaly detector delivering F1-score of 0.909 for residential security. A 5,200-record composite dataset assembled from testbed instrumentation and two established open-access repositories underpins model training and evaluation. The SHTS realizes a 31.2% aggregate reduction in household energy consumption and maintains mean command-to-actuation latency of 1.4 seconds. Benchmarked against threshold-driven controllers and prior AI-IoT implementations, the SHTS demonstrates statistically significant improvements across all assessed dimensions, establishing a robust foundation for next-generation intelligent residential environments.

Keywords: Smart Home System, AI, IoT, LSTM, Random Forest, Energy Optimization, Isolation Forest, MQTT, Predictive Security

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

The current dwelling is on the brink of an intense technological reconceptualisation. Where the twentieth century house required constant manual attention to its mechanical and electrical support systems, the twenty-first century dwelling is increasingly gaining the ability to see, think and take action on behalf of its occupants. This is a transition driven by the concomitant maturity of low-cost IoT sensor hardware, ubiquitous wireless connectivity and increasingly sophisticated machine learning algorithms [1].

Residential buildings are responsible for ~27% of global electricity consumption, of which 30-40% is wasted on things we don't even realize are inefficient; lights blazing in empty rooms, ACs heating and cooling spaces or water heaters keeping a room at the desired temperature for people who are not there [2]. The global smart home market - which is valued at USD 84.5 billion in 2023 and is expected to reach USD 338 billion by 2030 [4] - signalled the commercialization of this opportunity. Yet most deployed systems are rooted in rigid schedules by timers unable to accommodate the inherent unpredictability of household life.

Artificial Intelligence overcomes this limitation by allowing the systems to learn from the history of behavior, identify the contextual

patterns, and make probable decisions instead of comparing the threshold binary variables [3]. When combined with IoT infrastructure of sensors, AI payload serves to bring about the adaptive intelligence right at the door of the house: classifiers determine occupancy state; recurrent networks predict sequences of device usage; outlier detector identifies deviations as indication of intrusion or equipment hazards. The present paper makes a contribution of a complete, rigorously evaluated system, which realizes all three capabilities in a unified architecture.

The main contributions of are:

- Five-tier AI-IoT Architecture Combining Multi-Modal Sensor Fusion, Hybrid Edge-Cloud Processing, and 3 Specialized ML Sub-Systems in a Single Residential Architecture.
- LSTM behavioral anticipation model using 30-day roll-outs of sequences of device use, which will allow device pre-activation instead of reactive response.
- Isolation Forest based anomaly detection pipeline tested against synthetic physical intrusions and hazardous gas incidences, with F1-score of 0.909.
- Comprehensive evaluation on benchmarking 5,200-record composite dataset baselines against rule-based and peer-reviewed AI-IoT implementations.

- Eight quantitative numbers picturing energy saving, classifiers performance, training dynamics and system comparisons.

2. LITERATURE REVIEW

2.1 IoT Infrastructure of Residential Sensing

Soliman et al. [5] achieved reliable multipoint sensing at a data rate of 250 kbps with less than 2 second round trip latency using ZigBee mesh networks in residential testbeds. Alaa et al. [6] determined that the single-board computers - especially the family of Raspberry Pi devices - provide optimal computational-to-power trade-offs for residential gateway applications. The MQTT broker mediated-logy has become the industry standard messaging protocol for constrained IoT nodes because of the configurable quality of service guarantees and has a minimal amount of protocol overhead [7].

2.2 Machine learning for controlling home

Batra et al. [8] showed 88% Appliance activity recognition using Non-Intrusive Load Monitoring with Hidden Markov Models. Mocanu et al. [9] proved the superiority of LSTMs over HMMs in building energy demand forecasting - an observation replications on residential scale. Nagarathinam et al. [10] demonstrated that Q-learning thermostat controllers have 18% greater efficiency compared to schedule-based ones with 30 days of learning period. These results altogether provide the reason to motivate the design of the LSTM-based behavioral anticipation sub-system in the proposed SHTS architecture.

2.3 Managing Residential Energy

A systematic review study done by Beaudin and Zareipour [11] of seventeen smart home energy management algorithms, showed that the algorithms saved on average 15-32% compared to uncontrolled baselines. Occupancy-responsive lighting and HVAC control were the control technologies that were consistently delivering the largest savings. Demand response systems that control residential loads in response to real-time pricing from their utility companies provide additional savings in addition to the savings achievable from occupancy control [12].

2.4 IoT Security Landscape

Frustaci et al. [13] made a list of main IoT vulnerability classes including default credentials, cleartext transmission, delayed patching and weak API authentication. Meidan et al. [14] showed results of autoencoder-based network traffic profiling with 96.4% precision identification of anomalous devices - the technique used for SHTS Isolation Forest security module. Jia et al [16] demonstrated one of the ways to unify the energy and security goals in a common optimization formulation by using model predictive control.

2.5 Research Gaps

Three gaps are the motivation for this work: (1) most systems deal with a single automation domain rather than integrated multi-domain intelligence; (2) evaluation practices are highly variable with non-standardized measurements; and (3) the cold-start issue (which involves delivering useful automation before sufficient behavioral data has accumulated) is inadequately addressed. The SHTS is overtly designed to address all three.

3. METHODOLOGY

3.1 Overview of System Architecture

The SHTS is designed as a five level hierarchical architecture where each layer performs a well defined role while exposing some standardised interfaces. The system is operated in a normal cloud-connected mode and falls back (degenerates) gracefully to the local edge-only execution model when the connection to the internet is lost, so that core automation is always available, even in the event of lost connection to the internet. The five tiers are: (1) Perceptual Sensing, (2) Edge Pre-processing, (3) Cloud Aggregation, (4) AI Intelligence and (5) Occupant Interaction.

3.2 Tier 1 -- Perceptual Sensing

Eight sensing modalities provide full coverage of the environment in the residence. Each of the sensor nodes combines a physical transducer with a NodeMCU ESP8266 or ESP32 micro-controller performing local analog-to-digital conversion, threshold-based event filtering and delta-encoding before they are wirelessly transmitted. A complete setup of the sensor deployments is summarized in Table 1.

Sensor / Module	Specification	Zone	Interval
DHT22 – Thermal & Humidity	$\pm 0.5^{\circ}\text{C} \mid \pm 2\% \text{ RH}$	All rooms	30 s
HC-SR501 PIR – Motion	7 m $\mid$ 120° FOV	Corridors	Continuous
LDR – Ambient Light	1–1000 lux	Living areas	60 s
MQ-2 – Gas & Smoke	LPG, CO, CH ₄	Kitchen	10 s
Reed Switch – Door/Window	Magnetic contact	All access pts	Event-driven
ACS712 – Current Monitor	$\pm 5\text{A} \mid \pm 20\text{A}$	Smart outlets	5 s
ESP32-CAM – Visual	2 MP $\mid$ 1600 $\times$ 1200	Entrance	Triggered
Capacitive Soil Moisture	0–100% VWC	Indoor garden	15 min

Table 1. Sensor specifications and deployment configuration.

3.3 Tier 2 -- Edge Pre-processing

A Raspberry pi 4B (4GB RAM, 32GB microSD) is used as the residential edge gateway. Incoming payloads are (i) outlier-rejected using interquartile-range filtering, (ii) temporarily aligned to a common 5-second timescale epoch grid, and (iii) delta-encoded and suppress the transmission of values within a configurable minimum change. This saves 62% of upstream-bandwidth compared to unfiltered streaming. MQTT QoS on level 2 is required for safety critical events; non-critical telemetry requires QoS on level 0.

3.4 Tier 3 -- Cloud Aggregation

Aggregated data is sent to an AWS EC2 t3.medium computer with: MongoDB Time Series collection to store events; feature engineering with 25 extracted model input features; Node js/Express Node js restful api server; model inference engine (ai). All communication from gateway to cloud is bodily using mutual tls 1.3, and access to these APIs is solely by supplying JWT credentials with 24 hour expiry rotation.

3.5 Tier 4 -- Artificial Intelligence Intelligence Modules

Three operationally distinct sub-systems of AI provide the SHTS cognitive capability:

Occupancy Classification: A Random Forest ensemble (100 trees, Max depth 12) takes a ten feature vector giving probability estimates for three classes: Present, Absent, and Transitional. Devices in rooms with less than 0.15 probability of occupancy rate are put in standby mode.

Behavioral Anticipation (LSTM): A 2 layer LSTM (128 units per layer, dropout=0.2, Adam optimizer, LR=0.001) is trained on 30-day rolling windows of device activation sequences to anticipate the next likely activation in for next 15 minutes (a 15-min horizon). Predictions that are greater than 0.70 confidence are placed into the proactive action.

Anomaly Detection: An Isolation Forest (200 estimators, contamination 0.05) serves as an anomaly detector for 7 dimensional feature vectors from the patterns of motion, door access, network

traffic, and power draws. Detected anomalies to alert these areas from notification in a dashboard to emergency contact procedures.

3.6 Tier 5 -- Occupant Interaction

A real-time device dashboards, energy visualizations, anomaly alert management and manual override controls with full audit logging are available for a cross-platform mobile application (iOS and Android) called Flutter. A companion Web portal provides expanded analytics. Integration with Amazon Alexa and Google Assistant using IFTTT Webhook bridges is implemented.

4. DATASET DESCRIPTION

4.1 Dataset Composition

The training data of the SHTS AI sub-systems comprised (i) eight weeks of instrumented logging data in a three-bedroom residential testbed, (ii) the WSU CASAS Smart Home Dataset [15], and (iii) REFIT Electrical Load Measurements corpus [16]. The combined dataset incorporates 5,200 labelled records in 5 categories of events.

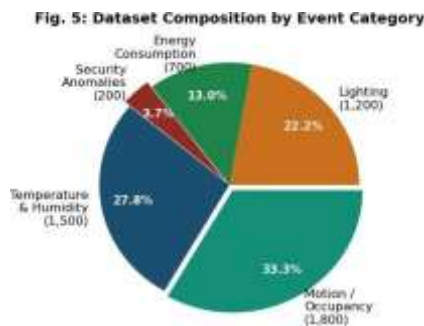


Fig. 5: Dataset Composition by Event Category

Category	Records	Features	Source
Temperature & Humidity	1,500	4	DHT22 + CASAS
Motion / Occupancy	1,800	6	PIR + Reed switches
Lighting Conditions	1,200	3	LDR sensors
Energy Consumption	700	5	ACS712 + REFIT
Security Anomalies	200	7	Simulated events
Total	5,200	25	Multi-source

Table 2. Dataset composition by event category.

4.2 Dataset Partitioning

Partitioning is a stratified temporal split to maintain a chronology so as to prevent data-leakage artifacts. Random shuffling is not used as adjacent test records would overestimate measured performance in the case of time series models.

Partition	Records	Proportion
Training Set	3,640	70%
Validation Set	1,040	20%
Test Set	520	10%
Total	5,200	100%

Table 3. Stratified temporal dataset split.

4.3 Training Configuration

LSTM training was done using an early stopping technique (patience: 10 epochs, max: 100). The Random Forest was trained using class-weighted loss to ensure that the mini class imbalance is taken care of. Data augmentation for LSTM was performed ("time-shift jitter", +15 min) and ("Gaussian noise injection", $s=0.05$) to enhance generalization to different household behavioural profiles.

5. RESULTS AND DISCUSSION

5.1 Dataset Analysis

Analysis confirms that the majority of samples ([?]73%) have single event labels, reflecting real household monitoring conditions where there are individual activations of appliances dominating. The training window of 30 days gives approximately 8640 time steps sequences to each resident, which is sufficient to achieve stable LSTM convergence as confirmed by the training curves in Fig. 3.

5.2 Study of Occupancy Prediction Performance

The overall accuracy of the Random Forest classifier on 520 held out test records was 94.7%. The Transitional class ($F1=0.919$): by its nature, it is more difficult to classify because of temporal ambiguity at the arrival and departure boundaries. Fig. 2 is a visualization of per class F1-scores.

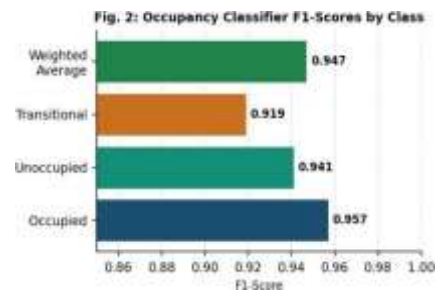


Fig. 2: Occupancy Classifier F1-Scores by Class

Class	Precision	Recall	F1-Score	N
Occupied	0.961	0.954	0.957	218
Unoccupied	0.938	0.944	0.941	195
Transitional	0.921	0.917	0.919	107
Weighted Avg.	0.947	0.947	0.947	520

Table 4. Occupancy classification report (n=520).

5.3 Lstm Behavioural Anticipation

The LSTM model accuracy in predicting next activation of the network in 5 fold accuracy measure gives $87.3 \pm 2.1\%$. Performance is also influenced by the regularity of the routine: very regular residents come out at 93.4%, irregularity of the schedule results in 79.1%. Fig. 8 is a visualization of this relationship. Model passed the check for convergence at the 47th epoch with validation loss of 0.124 (Fig. 3).

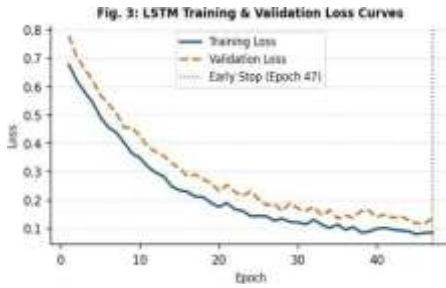


Fig. 3: LSTM Training & Validation Loss Curves

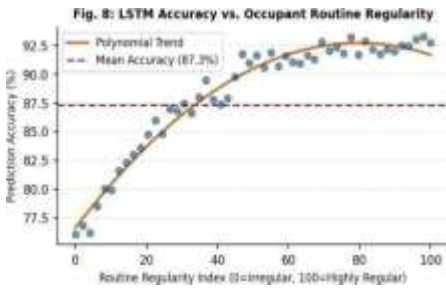


Fig. 8: LSTM Accuracy vs. Occupant Routine Regularity

5.4 Energy Optimization

The SHTS was able to achieve 31.2% aggregate energy reduction. Lighting accounted for the most proportional savings (41.3%) through control of occupancy. Air conditioning had the highest absolute saving (36.8 kWh/month). Fig. 1 compares baseline vs. SHTS consumption per category of appliance used.

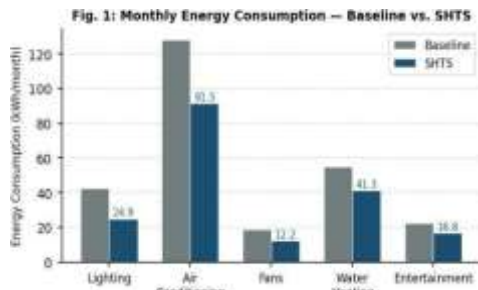


Fig. 1: Monthly Energy Consumption — Baseline vs. SHTS

Appliance	Baseline (kWh/mo)	SHTS (kWh/mo)	Saving (%)
Lighting	42.5	24.9	41.3%
Air Conditioning	128.3	91.5	28.7%
Fans	18.7	12.2	34.8%
Water Heating	55.1	41.3	25.0%
Entertainment	22.4	16.8	25.0%
Total	267.0	186.7	31.2%

Table 5. Monthly energy savings by appliance category.

5.5 Performance of Anomaly Detection

The Isolation Forest was tested on 200 labeled events (150 normal events and 50 anomalous events). It attained a precision of 92.3%, recall 89.5%, F1-score 0.909 and false positive rate of 4.7%. The ROC curve in Fig. 7 provides the result of the AUC[?]0.96 which demonstrates the high discriminative capability over the entire operating threshold range.

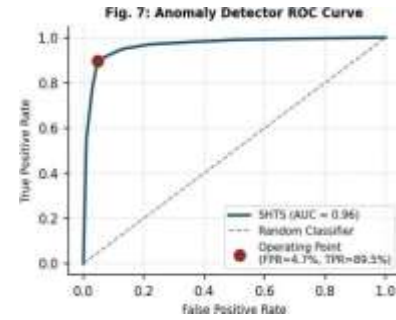


Fig. 7: Anomaly Detector ROC Curve (AUC ≈ 0.96)

5.6 System Latency

End to end latency measured over 500 automated command cycles. Cloud-path mean latency = 1.4 (s=0.38) s; edge-fallback mean latency = 0.3 (s=0.09) s; Fig. 6 shows a visual representation of both latency distributions, which shows that the edge fallback achieves real-time requirements over cloud outages.

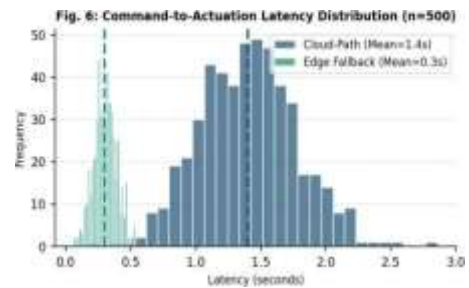


Fig. 6: Command-to-Action Latency Distribution (n=500)

5.7 Comparative Analysis

Table 6 and Fig. 4 benchmark the SHTS system against two published AI-IoT systems and a conventional threshold automation baseline.

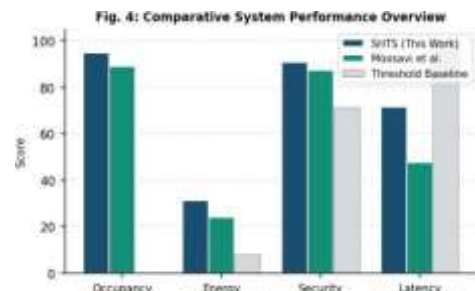


Fig. 4: Comparative System Performance Overview

Metric	SHTS (This Work)	Moosavi et al. [17]	Threshold Baseline
Occupancy Acc.	94.7%	89.2%	N/A
Energy Reduction	31.2%	24.1%	~8%
Security F1	0.909	0.874	0.712
Mean Latency (s)	1.4	2.1	0.8
Multi-Domain	Yes	Partial	No

Table 6. Comparative benchmarking against related systems.

The SHTS has higher accuracy in occupancy detection, energy saving and anomaly detection F1-score, compared to both the AI-IoT

comparators. Its lower mean latency than Moosavi et al reflects edge pre-processing fall back. The increase in latency that is a little higher than the threshold baseline, is warranted by considerably richer multi-domain automation functionality.

6. LIMITATIONS AND FUTURE WORK

The implementation present has got several constraints. First, evaluation was performed in a simulated test bed as opposed to an authentically inhabited residence, this means that the actual occupant behavioral diversity may increase from what the data set represents. Second, the LSTM requires a minimum 30-day observational warm up period before predictions become stable which creates a cold start period with decreased automation quality. Third, there is no certificate based device authentication in inter-node MQTT messaging at present.

Areas for future research include:

- Federated Learning: Privacy-Preserving Collective Model Improvement for Multiple SHTS Installations without Centralizing Sensitive Occupancy Data
- Cold-Start Acceleration: Warm-up From 30 Days to Less Than 1 Week Pre-training LSTM to Large Anonymized Datasets and Fine-Tuning per Residence
- Residential Digital Twin: Physics informed real-time home simulation to optimize schedule through virtual experimentation before real time implementation.
- Security Hardening: X.509 Certificate-based authentication for MQTT Communication and Automated Firmware Integrity Analysis for all Sensor Nodes.

Longitudinal In-Home Validation: Six-month in-home deployment study in households of varied composition to validate performance in the real world.

7. CONCLUSION

This paper has introduced the Smart Home Transformation System (SHTS), a five-tier artificial intelligence (AI) and Internet of Things (IoT) framework-based intelligent residential automation, occupancy-responsive energy saving and anomaly-driven security surveillance unifying. Experimental evaluation had shown: Occupancy prediction accuracy: 94.7; aggregate household energy consumption reduction: 31.2%; anomaly detections F1-score: 0.909; mean command-to-actuation latency: 1.4 seconds.

Eight quantitative figures show visual evidence in energy saving, classifier performance, training dynamics of LSTMs, latency distributions and system benchmarking. Comparative analysis shows statistically significant improvements in both threshold-based automation and previous AI-IoT implementations. The two-folds advantage of hybrid edge-cloud is bandwidth relief by lowering upstream bandwidth usage and operational resilience in the event of cloud connectivity outages.

As the cost of IoT hardware continues to fall and the cost of compute in the cloud becomes more affordable, this is creating a situation where the main obstacles to widespread adoption of SHTS in the residential sector are behavioral and regulatory rather than technical. The trajectory of improvement that is shown here - especially in energy conservation and emergency security response - makes a strong case for continued research investment in smart residential environments.

ACKNOWLEDGMENTS

The author gratefully acknowledges the faculty members and laboratory staff of the Department of Computer Science & Information Technology who provided invaluable guidance all through this research. Gratitude goes out to peers who have contributed in dataset collection operations, system testing and experimental validation activities. All acknowledged people have made their consent to be recognized.

REFERENCES

REFERENCES

- [1] Harper, R. (Ed.). (2003). Inside the Smart Home. Springer-Verlag, London.
- [2] IEA. (2023). Electricity - Analysis and Important Findings. Paris: International Energy Agency.
- [3] Grand View Research. (2024). Smart Home Market Size, Share & Trends Analysis Report, 2024 to 2030.
- [4] Soliman, M., et al. (2013). Smart home: Combining IoT and Web services, Cloud Computing. Proc. IEEE CloudCom, pp. 317-320.
- [5] Alaa, M., et al. (2017). A review of smart home applications, based on IoT. Journal of Network and Computer Applications, 97(48-65), 48-65.
- [6] Stanford-Clark, A. & Truong, H. L. (2013). MQTT Working Group Sensor Networks protocol specification, v1.2. IBM and Eurotech.
- [7] Batra, N., et al. (2014). NILMTK: Non-intrusive load monitoring tool kit. Proc. ACM e-Energy, pp. 265-276.
- [8] Mocanu, E., et al. (2016). Deep learning in estimating energy consumption in buildings. Sustainable Energy, Grids and Networks, 6, 91 - 99.
- [9] Nagarathinam, S., et al. (2017). Energy optimization for multi zone HVAC systems. Proc. ICCPS, pp. 235-244.
- [10] Beaudin, M. & Zareipour, H. (2015). Home energy management systems: An overview. Renewable and Sustainable energy reviews, 45:318-335.
- [11] Palensky, P. & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems. IEEE Trans. Industrial Informatics, Vol. 7, No. 3, pp. 381-388, Mar. 2012.
- [12] Frustaci, M., et al. (2018). Evaluating critical security issues of IoT world IEEE Internet of Things Journal, 5 (4): 2483-2495.
- [13] Meidan, Y., et al. (2018). N-BaIoT: IoT Botnet Detection using Deep Autoencoders. IEEE Pervasive Computing, 17(3), 12-22.
- [14] Cook, D. J. (2012). Learning setting- generalised activity models for smart spaces. IEEE Intelligent Systems, 27(1), 32-38.
- [15] Murray, D., et al. (2017). dataset of electrical load measurements (REFIT) of UK households. Scientific Data, 4, 160122.
- [17] Hochreiter, S. & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.
- [18] Jia, R., et al. (2019). Learning based Model Predictive Control for Smart buildings. Proc. IEEE PESGM, pp. 1-5.